Managing User and Cloud Service Provider Access to Data in Cloud Computing- Panacea for Data Vulnerability.

Uchechukwu P. Emejeamara [1], Udochukwu J. Nwoduh [2], and Andrew Madu[3]
[1]*Research Scholar, Dept. Computer Science, University of Bridgeport, CT, USA.*
[2]*Lecturer, Dept. Computer Science, Federal Polytechnic Nekede, Owerri, Nigeria*.
[3]*Lecturer, Dept. Computer Science, Federal Polytechnic Nekede, Owerri, Nigeria*.

***Abstract*— The cloud computing technology allows organizations and individuals to share infrastructure, which reduces the cost of conducting business operations. The large number of security threats associated with cloud computing discourages some organizations and individuals from adopting this technology. The key types of security risks can be put into three categories, including network-related, data, and cloud environment threats. The cloud environment threats include denial of service and account hijacking. Data threats include the loss or breach of critical information. The network-related sources of threat include malicious insiders, abuse of cloud services, and insecure interface APIs. Segregation of duties and effective recruitment procedures are some of the key strategies that should be used to manage administrators' access to data. The users' access to the data can be managed through the application of configuration management tools, manual control of servers, enterprise-identity solution, exposure of AD and LDAP to the internet, and directory-as-a-service.**

***Index Terms*— Cloud computing, security risks, data threats, cloud servers, user management.**

I. INTRODUCTION

Technological advancement has affected nearly all aspects of human life. Organizations and individuals adopt the modern technology for different reasons, including the need to enhance efficiency in their day-to-day work and minimize the cost of doing business. Cloud computing is one of the most promising technologies in terms of cost reduction in the contemporary business environment. Most of the benefits (such as a reduction in cost) associated with cloud computing technology are attributed to the possibility of sharing resources and infrastructure among the users [1]. Although cloud computing has become a popular topic in the information technology sector, the key security threats associated with it are likely to discourage many organizations that would like to apply the new innovation in their businesses. The purpose of this research paper is to identify strategies that can be used to manage user and cloud administrators' access to cloud and data.

II. THE KEY VULNERABILITIES OF CLOUD COMPUTING TECHNOLOGY

While cloud computing has become a household name in the field of technology, accountability, vulnerability, and the level of security are key terms that cannot be avoided in any discussing involving the application of the new innovation [2]. Organizations as well as individuals who chose to adopt the technology experience unique security threats. In order to identify the key strategies that can be used to manage how users and administrators access clouds and data, it is important to comprehend the major types and sources of vulnerabilities. The key security risks associated with the new technology are put into three groups, namely network-related, data, and cloud environment threats.

A. Cloud Environment Threats

1. Denial of service

Denial of Service (DOS) is a unique type of cyber attack that involves the prevention of legitimate users from accessing the database, cloud, or other related services. This type of threat affects about 81 % of the users of the cloud computing services [3]. In most cases, DOS is done by malicious users of the cloud with technological skills that allow them to take advantage of the weak areas left by the cloud service provider. The attack involves a compromise on the service that is used to consume the large percentage of the cloud's memory, network bandwidth, and the computational power. This complication reduces the capacity of the cloud to respond to commands made by genuine users. The DoS is largely attributed to the lack of accountability on the part of the service provider.

2. Account and service hijacking

Hijacking of services takes place when an authorized person gains access to the cloud or an account owned by another person, which is accomplished by stealing the credentials of the genuine users. These credentials can then be used to compromise the account of the affected individual and other users who rely on the same cloud [3]. The vulnerability can result from failures on the part of the cloud users or providers. In most cases, successful attackers eavesdrop on users' operations, redirect the entire network traffic, and modify the data.

B. Data Threats

1. Data loss

Data loss is among the most significant types of vulnerability that discourage many organizations that would like to adopt cloud computing technology. It is estimated that over 44 % of all organizations that have started using cloud computing have suffered from incidents of data loss at least once [3]. The occurrence of data loss is attributed to different factors, including the loss of encryption keys, faults that take place in the storage system, malicious attacks, natural disasters, deletion, and corruption. In some cases, malware programs have been used to target different cloud operations. Based on this analysis, it is evident that most of the vulnerabilities (such as faults in the storage systems) that lead to the loss of data are associated with the lack of accountability on part of the service provider.

2. Data breaches

Data breach takes place when sensitive information about a customer or an origination leaks and gets into the hands of an unauthorized person. Most cases of data breach are perpetrated by individuals with the intention of accessing sensitive information that can lead to the destruction of an organization or enhance the attacker's ability to access critical services. The key factors that increase the risk of data breach include flaws in the cloud infrastructure, operational issues, insufficient authentication, and the lack of audit controls [4]. These sources of vulnerability result from the lack of accountability on the part of the organizations that provide cloud computing services. However, there are some instances when malicious users apply virtual machine (VM) to break through the cloud system and access the data.

C. Network-Related Sources of Vulnerability

1. Malicious insiders

Cloud infrastructure is maintained by individuals who have access to the entire of the cloud. These administrators are employed by organizations that provide cloud computing services and given the responsibility of managing the entire environment. Unfortunately, some administrators have malicious intentions and they can easily access user's data and resources to accomplish their selfish interests [5]. The malicious insiders use different cloud applications, network, and data to engage in unprivileged activities. Other categories of malicious insiders include hobbyist attackers who access sensitive information for fun and corporate espionage persons who are mostly sponsored by governments or competitors.

2. Abuse of the cloud services

The abuse of services occurs when users of the cloud engage in activities that are unethical and illegal. They tend to contravene the terms and conditions set by provider. This type of threat results from individuals who have legitimate access to the cloud, but they abuse it by taking advantage of the existing vulnerabilities to engage in authorized activities, such as gaining access to data stored by other users. It is estimated that about 84 % of the cloud users consider the abuse of cloud services as one of the key threats that make them reconsider the idea of using the new technology [3]. This threat is attributed to the lack of the provider's capacity to screen every user who subscribes to the cloud.

3. Insecure interface and APIs

The communication between the internet and the software is defined by the Application Programming Interfaces. These interfaces can, at times, serves as sources of security risk in cloud computing. The role of the APIs is to facilitate the management of cloud infrastructure and enhance the accessibility of the data. Providers of the cloud services give organizations that use their infrastructure APIs in order to help them deliver services to their clients. The development of weak APIs increases the cloud's vulnerability since the critical information and keys can be accessed by the third party users [3]. The third party users who have the keys can access encrypted data stored by other customers, which reduces the integrity as well as the confidentiality of the cloud.

III. THE MANAGEMENT OF ADMINISTRATORS' ACCESS TO DATA

Cloud administrators play a vital role in ensuring that the systems are working as expected in order to help users be more efficient and effective. However, they pose a great threat to the integrity of the cloud, given that they have access to all data and personal details of the users, which can be misused. However, this challenge can be addressed through an effective management of administrators' access to the cloud and the data [5]. The focus of the organizations that offer cloud computing services should be to implement strategies that will ensure that administrators with malicious intentions are unable to access critical information stored by users. There are three key strategies that cloud providers can use to enhance effectiveness in the management of administrators' access to the cloud, which include the development of effective access controls, segregation of duties, and screening of employees during recruitment.

A. Development of Effective Access Controls

Although cloud administrators require adequate access to infrastructure in order to carry out their mandates, effective controls should be put in place. The purpose of these controls is to ensure that the administrators are only able to access data as well as infrastructure for which they have been authorized [3]. For example, organizations that offer cloud computing services can limit the privileges of their administrators by allowing them to access specific accounts. This goal can be achieved by ensuring that each administrator can only manage identified user accounts, not virtually everything that is stored in the cloud. In addition, administrators should be required to use specific login details that can be traced later in order to assess their access and usage of the cloud infrastructure.

B. Segregation of Duties

The purpose of segregating the duties is to ensure that one function is not carried out by a single administrator from the start to the end. The effectiveness of this strategy is attributed to the fact that no single administrator has a full control of the entire cloud or the data stored by a given user [6]. In addition, it is easier for the management teams to trace administrators who abuse their privileges when each one of them is assigned specific duties. By segregating the duties, cloud providers limit the privileges and powers of individual administrators, which in turn reduce their capacity to abuse data and infrastructure in a way that could be a security threat to users.

A case study of Microsoft's Azure Cloud infrastructure indicated that administrative functions can be segregated and put into five groups. First, billing administrators are mandated to purchase packages and manage users' subscription [6]. Secondly, global administrators are given the roles of managing domains, licensing rights, and multifactor authentication. Third, password administrators manage login details of all users and how they are changed. They also manage the subscription rights of users, but they have no control over the billing process. Fourth, service administrators play the role of maintaining requests for different cloud services. They also monitor the process of delivering those services to clients. Lastly, the cloud management administrators are given the mandate of resetting passwords and managing users in general.

C. Effective Recruitment Procedures and Screening of Administrators

The cloud providers should put in place effective mechanisms to ensure that all individuals who are given the role of managing the system are trustworthy. This objective can be achieved by using recruitment procedures that enable the cloud providers to screen candidates who apply the administrative job positions. The recruitment process should be thorough in order to reduce the chances of job applicants with malicious intents from joining the cloud provider's workforce. Some scholars have identified that making the behavior of members of staff part of legal requirements in a contract between them and the cloud provider can go a long way in reducing the risk of malicious engagements [3]. The objective of developing effective recruitment and screening procedures is to reduce security threat caused by malicious insiders.

IV. MANAGEMENT OF USER'S ACCESS TO THE CLOUD AND THE DATA

A. Challenges of Managing User Access

Cloud providers and users have experienced the benefits and challenges of this technology in equal measures. The primary goal of establishing a cloud is to reduce the need for individual companies to invest in their own infrastructure. Therefore, the cloud allows millions of users to share resources in carrying out critical functions, such as data storage and analysis [1]. The large number of individuals and organizations that are allowed to share the cloud is a security risk since providers find it difficult to monitor activities of millions of users. However, there are several strategies that can be used to

manage users in order to minimize the risk of the data breach and loss of information.

B. Configuration Management Tools

Configuration management tools (such as Puppet and Chef) help providers to create and manage users through scripts. Cloud providers use these tools by popping users into a boom and the script, and then putting them into their server [7]. Providers can then drop in the users' public keys. This strategy is preferred when provider is using Infrastructure-as-a-Server (IaaS) frameworks, including Rackspace and AWS. These configuration tools allow providers to take control over activities that are carried out by users on their cloud platforms. In addition, the effectiveness of configuration tools reaches the maximum point when the number of users under the management of the provider is relatively small.

C. Manual Management of Cloud Server and Users

Although automation of systems is associated with an increase in the level of efficiency, it causes some security risks since cloud providers may not know the credibility of users who subscribe to their systems. Fully automated cloud systems increase security threat by allowing users to sign up on their own and without any intervention of the cloud providers [7]. The challenges associated with this approach can be addressed through the manual management of users. The manual management approach allows cloud providers to log into the servers, manage the entire process of user creation, facilitate account modification, handle termination process, and communicate with users directly. This approach makes it possible to manage users case by case, which limits the probability of malicious individuals and organization gaining access to the cloud. Therefore, all users within a cloud that is managed manually by providers are secure. However, this approach is more effective when the number of users is relatively small.

D. Implementation of an Enterprise-Class Identity User Management Solution

The enterprise-class identity management solution is recommended for large corporations with cloud systems that are accessed by a large number of users. It involves the installation of user management systems on-premises. These systems are then connected to the main directory store [8]. Agents are then installed on every device that is used to access the cloud or the data stored in it. The successful adoption of this user management solution requires the intervention of vendors, who provide professional services. The enterprise-class identity user management is a flexible solution that allows providers to monitor clients who use a wide variety of devices, including mobile phones and desktops. It can also be used in the management of internal cloud servers, where providers install agents onto them. This installation enables them to talk back to the main-on-premise server [8]. Although this solution is considered as one of the most effective options for the management of cloud users, it is costly, which makes it inaccessible to small organizations.

E. Exposing AD And LDAP to the Internet

The exposure of active directory (AD) and lightweight directory access protocol (LDAP) to the internet allows the server to communicate to user directories directly. However, adequate security measures should be put in place before this exposure is done [8]. Additional configuration and security interventions allow the servers to talk to specific servers, which reduces the chances for unauthorized persons to access the cloud and abuse. This technology allows cloud providers to limit the number of users who can access their infrastructure. Failure to include additional security measure when exposing the AD and LDAP to the internet makes the directory available to anyone, which lowers the level of security and confidentiality of other users.

F. Directory-as-a-Service

A cloud-based directory links on-premises AD to the infrastructure. The cloud provider can leverage the directory-as-a-service (DaaS) as a viable solution for the management of users. A lightweight agent that is placed on user's store has the capacity to synchronize users to the provider's cloud-based directly [9]. This allows the cloud servers to talk directly to DaaS and authenticate access. The technology is safe because the DaaS is located in the cloud, which implies that there is no networking required. Servers are able to communicate to the directory via an agent installed on each one of them or a secure connection. The level of security is further enhanced by the fact that user changes are managed in one place, which is the internal directory. These changes are then propagated via the cloud directory and each of the servers. Some of the key benefits of this user management solution include the high level of security, availability, and simplicity.

V. CONCLUSION

Cloud computing is a significant type of technological advancement that has helped companies and individuals to reduce the cost of doing business. However, it has come with an equal share of challenges. The possibility of sharing infrastructure is among the key factors that have attracted many individuals and organizations towards this new technology. The large amount of crucial data that is stored in the cloud increases the vulnerability of users. Hackers and other individuals with malicious intentions target the clouds since a successful attack helps them access useful data. The high level of vulnerability of clouds can be attributed to different factors, including failures on the part of the users and providers to take the necessary security measures. This challenge calls for effective management of the administrators and users of the cloud in order to minimize the levels of exposure of the infrastructure and the data stored in the clouds.

REFERENCES

[1] K, Kavitha, Study on cloud computing model and its benefits, challenges, *The International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, no. 1, pp. 2423-2430, 2014.

[2] T. Chou, Security threats on cloud computing vulnerabilities, *International Journal of Computer Science and Information Technology*, vol. 5, no. 3, pp. 79-88, 2013.

[3] M. Kazim and S. Zhu, A survey on top security threats in cloud computing, *International Journal of Advanced Science and Application*, vol., 6, no. 3, pp. 109-113, 2015.

[4] M, Khalil, A, Khreishah, and M, Azeem, Cloud computing security: A survey, *Computers*, 3, pp. 1-35, 2014.

[5] A, Mahajan, and S, Sharma, The malicious insiders threat in the cloud, *International Journal of Engineering Research and General Science*, vol. 3, no. 2, pp. 245-256, 2015.

[6] V, Lazarova, Managing access to cloud services by administrators in the company, *Business Economic Journal*, vol. 7, pp. 1-3, 2016.

[7] D, Armstrong, D, Espling, J, Tordsson, K, Djemame, and E, Elmroth, Contextualization: Dynamic configuration of virtual machines, *Journal of Cloud Computing Advances, Systems, and Applications*, vol.4, no. 17, pp. 1-15, 2015.

[8] S, Eludiora, O, Abiona, A, Oluwatope, A, Oluwaranti, C, Onime, and L, Lawrence, A user identity management protocol for cloud computing paradigm, *International Journal of Communications, Network, and System science*, vol. 4, pp. 152-163. 2012.

[9] W, Abdullahi, A, Babate, and A, Jakwa, Cloud computing: Technical, non-technical and security issues, *International Journal of Computer Applications Technology and Research*, vo. 3, no. 3, pp. 169-175.